訂正有り

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　昭64－81087

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和64年(1989)3月27日
G 06 K 17/00		S－6711－5B E－6711－5B	

審査請求　未請求　発明の数 1　(全4頁)

㊹発明の名称　ICカードデータ伝送方式

㉑特　願　昭62－238207
㉒出　願　昭62(1987)9月22日

㉗発明者　落合　誠　大阪府茨木市丑寅1丁目1番88号　日立マクセル株式会社内
㉑出願人　日立マクセル株式会社　大阪府茨木市丑寅1丁目1番88号
㉔代理人　弁理士　梶山　佶是　外1名

明　細　書

1.発明の名称　ICカードデータ伝送方式

2.特許請求の範囲

(1) ICカードと、このICカードが装着される情報処理装置との間でなされるICカードデータ伝送方式において、前記情報処理装置と前記ICカードのうち少なくとも一方は、伝送情報の暗号処理に関する複数の暗号化処理情報と、この暗号化処理情報に基づいて送信データを暗号化する暗号器とを備え、前記情報処理装置と前記ICカードのうち少なくとも他方は、複数の前記暗号化処理情報に関する解読器を備え、前記一方は、前記暗号器により暗号化した前記送信データを送信情報とし、この送信情報にその暗号化処理情報を付加して情報を送出し、前記他方は、付加された前記暗号化処理情報を受け、受けたこの暗号化処理情報に基づき前記送信データを前記解読器により解読して復元することを特徴とするICカードデータ伝送方式。

3.発明の詳細な説明

[産業上の利用分野]

この発明は、ICカードデータ伝送方式に関し、詳しくは、ホストコンピュータとか、ICカードリーダ・ライタ等の外部装置とICカードとの間で暗号化してデータを伝送する場合において、送信データに対するセキュリティを向上させることができるようなICカードデータ伝送方式の改良に関する。

[従来の技術]

ICカードに対する従来のデータ伝送方式は、一般に、データがそのまま転送されて送受信され、暗証番号等については、ICカード内部でスクランブル変換されることもあるが、データ自体の暗号化は行わない場合が多い。データ自体の暗号化を行う場合にも、暗号化方式を指示するためのコマンドが必要とされ、あらかじめ定められた特定の暗号化方式が採用される。

このような暗号化としては、例えば、取引等の一連の処理を行う時などには、コマンド群及びレスポンス群が処理を行うに先立って指定した暗号

化方式に従って処理され、外部装置もＩＣカードも同一の暗号化方式に従ってデータ伝送を行う。

しかし、このような方式では、その暗号化方式が一度他人に解析されてしまえば、一連のデータを抽出して解読することが容易となり、セキュリティが低いという欠点がある。

［解決しようとする問題点］

この発明は、前記のような従来方式が持っているデータ伝送時のセキュリティの低さを向上させ、又はその記憶情報に対してセキュリティの高いＩＣカードを実現できるＩＣカードデータ伝送方式を提供することを目的とする。

［問題点を解決するための手段］

このような目的を達成するためのこの発明のＩＣカードデータ伝送方式における手段は、ＩＣカードと、このＩＣカードが装着される情報処理装置との間でなされるＩＣカードデータ伝送方式において、情報処理装置とＩＣカードのうち少なくとも一方は、伝送情報の暗号処理に関する複数の暗号化処理情報と、この暗号化処理情報に基づいて送信データを暗号化する暗号器とを備えていて、情報処理装置とＩＣカードのうち少なくとも他方は、複数の暗号化処理情報に関する解読器を備えていて、一方は、暗号器により暗号化した送信データを送信情報とし、この送信情報にその暗号化処理情報を付加して情報を送出し、他方は、付加された暗号化処理情報を受け、受けたこの暗号化処理情報に基づき送信データを解読器により解読して復元するものである。

［作用］

このように構成することにより、例えば、外部装置がデータの送信を行うコマンド列又はＩＣカードから受信するレスポンス列の中に、そのコマンド列又はレスポンス列で伝送するデータに対する暗号化の方式を示すコードを付加し、そのコードに従ってＩＣカード又はＩＣリーダ・ライタ等の外部装置がデータの送受信を行うことになるので、コマンド単位での暗号化を行うことが可能である。

その結果、１つのコマンドの暗号化方式を解読されても次のコマンドは、別の暗号化方式を採ることができる。そこで、データ伝送時にデータを抽出される危険性が少なくなる。また、ＩＣカード側では、その記憶情報に対してセキュリティの高いＩＣカードを実現できる。

［実施例］

以下、この発明の一実施例について図面を参照して詳細に説明する。

第１図（ａ）は、この発明を適用したＩＣカードデータ伝送方式の一実施例を示すブロック図、第１図（ｂ）は、その伝送情報のフォーマットの説明図である。

第１図（ａ）において、１は、ＩＣカード２が装着され、ＩＣカード２とデータの授受を行うＩＣカードリーダ・ライタであり、これらは、通常、コネクタで接続されるか、コイル等を介して電磁結合され、被接触状態で接続される。

３は、ＩＣカードリーダ・ライタ１からＩＣカード２に対して送出されるコマンド列であり、４は、このコマンド列３に対するＩＣカード２からのレスポンス列である。

コマンド列３とレスポンス列４のフォーマットの詳細は、第１図（ｂ）に示すように、その先頭部分に先頭を示す開始コード１１が設けられ、次にコマンドコード又はレスポンスコード１２、そして暗号化コード１３、送信データ１４、最後に終了コード１５と続く構成となっている。

ここで、暗号化コード１３は、ＩＣカードリーダ・ライタ１とＩＣカード２に記憶されたそれぞれの暗号化コードテーブル５から選択されるものであって、この暗号化コードテーブル５には、複数の暗号化コードが記憶されている。

前記コマンド列３とレスポンス列４の暗号化コード１３はこれらのうちから選択された１つであり、ＩＣカードリーダ・ライタ１とＩＣカード２には、暗号化コードテーブル５に記憶された暗号化コードに基づいて送信データを元の情報に戻す解読器６と、送信データを暗号化する暗号器７とがそれぞれ設けられている。

暗号器７は、例えば、選択した暗号化コード１

3と送信データとを掛けてその答え求め、これを暗号化した送信データ14とするものとか、暗号化コード11と送信データとを特定の関数でスクランブル処理して暗号化して送信データ14を得るもの、さらに、暗号化コード11に対応する暗号化関数自体を選択して、選択した関数により送信データを暗号化して暗号化した送信データ14を得るもの等、各種の暗号化処理機能のうちの1つを採用したものである。

なお、この暗号器7で使用されるその時々の暗号化コードは、暗号化コードテーブル5に記憶されているものであり、そこから読出されて、暗号器7に加えられる。そして、暗号器7に加えられたその時の暗号化コードが暗号化コード13として暗号化された伝送データ14とともに送信時のコマンド列3又はレスポンス列4として送られる。

送信側で選択する暗号化コード13は、暗号化コードテーブル5の暗号化コードから選択されるものであるが、その選択は、それぞれのマイクロプロセッサによりランダムに選択するほうがよい。しかし、特定のルールに従って選択するようにしてもよい。

一方、解読器6は、受信した暗号化コード13を使用して前記暗号器7の処理とは逆の処理を行い、送信データ14から元の送信データを復元するものである。

このような送受信方式おいて、ICカード2を用いてショッピング等を行う場合には、ICカードリーダ・ライタ1とICカード2との間でコマンド列3及びそのコマンド列3に対するICカード2のレスポンス列4の送受信を必要なだけ行う。この時のコマンド列3及びレスポンス列4の中の送信データ14は、その都度、暗号化コード13で示す暗号化方式に従い暗号化された形式で伝送されることになる。

これを受信した側では、暗号化コード13に従い、送信データ14を処理し、送信データ14を通常の形式に復元する。この場合、この暗号化コード13は、1つのコマンド列3及びレスポンス列4の中でのみ有効であり、次のコマンドを送る時には、別な暗号化コード13がセットされることになる。なお、この場合に、ある回数同じ暗号化コードが使用されて、変更されてもよいことはもちろんである。

したがって、1つのコマンドの暗号化方式を解読されても、次のコマンドでは、また別の暗号化方式となるか、別の暗号化方式を指定できるので、データ伝送時のデータ盗用に対するセキュリティを向上させることができる。

ところで、実施例では、ICカードとICカードリーダ・ライタ双方に暗号器と解読器、複数の暗号化コード（暗号化コードテーブルとして、なお、テーブルでなくもよい）とを設けているが、ICカード側に暗号器と複数の暗号化コードとを設け、ICカードリーダ・ライタ側にこれに対する解読器を設ければ、ICカードのセキュリティが保証されるので、十分である。また、データ伝送時のセキュリテイを向じさせるには、前記とは逆に、ICカードリーダ・ライタ側に暗号器と複数の暗号化コードとを設け、ICカード側にこれに対する解読器を設ければ、十分である。

なお、解読器とか暗号器は、マイクロプロセッサとその処理プログラムとにより実現されても、専用の特別なハードウエアで実現されてもよく、その方法を問うものではない。

実施例では、ICカードをICカードリーダ・ライタに装着した例を上げているが、これは、ICカードリーダ・ライタに限定されるものではなく、ホストコンピュータ等に直接接続されてもよく、ICカードの送受信の相手は、ICカードが装着される情報処理装置一般でよいことはもちろんである。

[発明の効果]

以上説明したように、この発明にあっては、データの送信を行うコマンド列又は受信を行うレスポンス列等の送信情報の中に、その送信情報で伝送するデータに対する暗号化の方式を示す暗号化コードを付加し、この暗号化コードに従ってICカード又はそれが装着される情報処理装置がデータの送受信を行うようにしているので、送信情報

単位での暗号化を行うことができる。

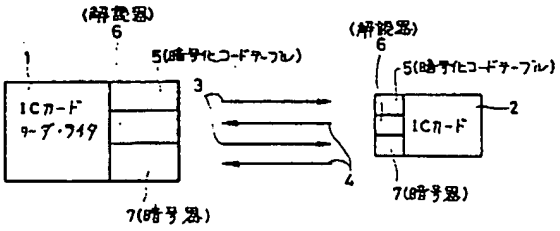
その結果、１つの送信情報の暗号化方式を解読されても次の送信情報が別の暗号化方式を採ることができ、データ伝送時に、データを読み出される危険性が少なくないデータ伝送方式が実現できる。また、ＩＣカード側では、その記憶情報に対してセキュリティの高いＩＣカードを実現できる。

4.図面の簡単な説明

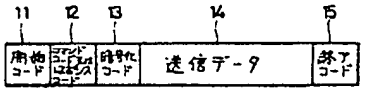
第１図（ａ）は、この発明を適用したＩＣカードデータ伝送方式の一実施例を示すブロック図、第１図（ｂ）は、その伝送情報のフォーマットの説明図である。

１…ＩＣカードリーダ・ライタ、
２…ＩＣカード、３…コマンド列、
４…レスポンス列、５…暗号化コードテーブル、
６…解読器、７…暗号器、１１…開始コード、
１２…コマンドコード又はレスポンスコード、
１３…暗号化コード、１４…送信データ、
１５…終了コード。

第１図(a)



第１図(b)



【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成６年（１９９４）１２月６日

【公開番号】特開平１－８１０８７
【公開日】平成１年（１９８９）３月２７日
【年通号数】公開特許公報１－８１１
【出願番号】特願昭６２－２３８２０７
【国際特許分類第５版】
G06K 17/00 S 7459-5L
E 7459-5L

手続補正書（自発）

平成６年６月２９日

特許庁長官殿

１．事件の表示
特願昭６２－２３８２０７号
２．発明の名称
ICカードデータ伝送方式
３．補正をする者
事件との関係　特許出願人
住所　大阪府茨木市丑寅一丁目１番８８号
名称　（５８１）日立マクセル株式会社
代表者　渡邉宏
（連絡先　電話0726-20-5127 知的財産部）
４．補正命令の日付　自発
５．補正により増加する発明の数　なし
６．補正の対象
（１）願書の発明の名称の欄
（２）明細書の発明の名称の欄
（３）明細書の特許請求の範囲の欄
（４）明細書の発明の詳細な説明の欄
７．補正の内容
別紙のとおり

（１）願書の発明の名称の欄を「ICカードシステム」に補正する。
（２）明細書の発明の名称の欄を「ICカードシステム」に補正する。
（３）明細書の特許請求の範囲の欄を次のように補正する。
「（１）ICカードと、このICカードが装着されデータの書き込み、読み出しをおこなう情報処理装置とから構成されるICカードシステムにおいて、
前記情報処理装置と前記ICカードのうち少なくとも一方は、伝送情報の暗号処理方式に関する複数の暗号化処理情報と、複数の暗号化方式の中から前記暗号化処理情報に基づいた暗号化方式により送信データを暗号化する暗号器とを備え、
前記暗号器により暗号化した前記送信データに暗号化処理情報を付加したデータを他方に送信し、
前記情報処理装置と前記ICカードのうち少なくとも他方は、前記暗号器に対応する解読器を備え、
受信したデータに含まれる前記暗号化処理情報に基づいた解読方式にて、前記送信データを前記解読器により解読して復元することを特徴とするICカードシステム」
（４）明細書第２頁第２行の「この発明は、」から第２頁第８行の「に関する。」を次のように補正する。
「この発明は、ホストコンピュータやICカードリーダ・ライタ等の情報処理装置とICカードから構成されるICカードシステムに関し、詳しくは、情報処理装置とICカードとの間で暗号化してデータを転送する場合において、送信データに対するセキュリティを向上させることができるICカードシステムに関する。」
（５）明細書第３頁第１０行から３頁第１１行の「ICカードを実現できるICカードデータ伝送方式」を「ICカードシステム」に補正する。
（６）明細書第３頁第１４行の「このような目的を」から第４頁第９行の「復元するものである。」を次のように補正する。
「このような目的を達成するため、本発明は、ICカードと、このICカードが装着されデータの書き込み、読み出しをおこなう情報処理装置とから構成されるICカードシステムにおいて、前記情報処理装置と前記ICカードのうち少なくとも一方は、伝送情報の暗号処理方式に関する複数の暗号化処理情報と、複数の暗号化方

式の中から前記暗号化処理情報に基づいた暗号化方式により送信データを暗号化する暗号器とを備え、前記暗号器により暗号化した前記送信データに暗号化処理情報を付加したデータを他方に送信し、前記情報処理装置と前記ICカードのうち少なくとも他方は、前記暗号器に対応する解読器を備え、受信したデータに含まれる前記暗号化処理情報に基づいた解読方式にて、前記送信データを前記解読器により解読して復元するものである。」

（７）明細書第５頁第９行から５頁第１０行の「ICカードデータ伝送方式」を「ICカードシステム」に補正する。

（８）明細書第８頁第１７行の「接接触状態」を「非接触状態」に補正する。

（９）明細書第１１頁第４行の「データ伝送時に」から第１１頁第７行の「実現できる。」を「データ転送及び、ICカードの記憶情報に対してセキュリティの高いICカードシステムを実現できる。」に補正する。